CLAIMS

WHAT IS CLAIMED IS:

1. A method for generating filters based on data entering a network device, comprising:

separating the data into different network flows;

analyzing at least one of said network flows;

detecting potentially harmful network flows; and

generating a filter to prevent packets corresponding to said detected potentially harmful network flows from passing through said network device.

2. The method of claim 1 further comprising refining said filter to reduce the amount of packets that are filtered.

3. The method of claim 1 wherein separating data into different flow comprises classifying network flow based on a source device sending a packet.

4. The method of claim 3 wherein the network flow is classified based on an IP address of the source device.

5. The method of claim 1 wherein separating data into different network flows comprises performing a lookup in a flow cache.

6. The method of claim 1 wherein analyzing at least one of said network flows comprises monitoring statistics associated with said network flows.

7. The method of claim 1 further comprising propagating the generated filter to an upstream network device.

8. The method of claim 1 wherein separating the data into different network flows is performed by hardware and analyzing said network flow is performed by software.

9. The method of claim 1 further comprising sending flow records corresponding to each of said network flows to a flow analyzer operable to analyze said network flows.

10. The method of claim 9 wherein the flow analyzer comprises software.

11. The method of claim 1 further comprising selecting a class of said network flows to analyze based on previously analyzed network flows.

12. The method of claim 1 wherein said potentially harmful network flows include denial of service attacks.

13. The method of claim 1 wherein said potentially harmful network flows include a high rate of incoming packets.

14. The method of claim 1 wherein detecting potentially harmful network flows comprises identifying a source address associated with said harmful network flow and generating a filter comprises generating a filter to prevent packets from said identified source from passing through said network device.

15. A computer program product for generating filters based on analyzed network flows, comprising:

code that analyzes said network flows;

code that detects potentially harmful network flows;

code that automatically generates a filter to prevent packets corresponding to said detected potentially harmful network flows from passing through the network device; and

a computer-readable storage medium for storing the codes.

16. The computer program product of claim 15 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave.

17. The computer program product of claim 15 further comprising code that propagates said filter to an upstream network device.

18. A system for automatically generating filters based on data entering a network device, comprising:

a netflow device operable to receive streams of packets, separate said streams, and create a summary record containing information on each of said streams;

a flow analyzer operable to analyze said records and identify potentially harmful network flows; and

a filter generator operable to generate a filter to prevent packets corresponding to said identified potentially harmful network flows from passing through the network device.

19. The system of claim 18 wherein the network device comprises hardware and the flow analyzer and filter generator comprise software.

20. The system of claim 18 wherein the network device comprises an ACL classifier, a lookup device, and a plurality of flow buckets.

21. The system of claim 18 further comprising a filter propagator operable to send information on said filters to an upstream device and request the upstream device to create a corresponding filter.

22. A system for automatically generating filters based on data entering a network device, comprising:

means for separating the data into different network flows;

means for analyzing at least one of said network flows;

means for detecting potentially harmful network flows; and

means for generating a filter to prevent packets corresponding to said detected potentially harmful network flows from passing through the network device.